SETA

Deliverable 8.2

Security Requirements for the SETA Technology

Grant Agreement number:	688082
Project acronym:	SETA
Project title:	An open, sustainable, ubiquitous data and service ecosystem for efficient, effective, safe, resilient mobility in metropolitan areas
Funding Scheme:	H2020-ICT-2015

Authors

Danilo Massa — danilo.massa@aizoongroup.com
Enrico Magnarello — enrico.magnarello@aizoongroup.com

Internal Reviewer

Luca Bolognini — luca.bolognini@aizoongroup.com
Marcin Sieprawski — marcin.sieprawski@softwaremind.pl

State: Final
Distribution: Public

Deliverable History

Date	Author	Changes
17-03-2016	Massa, Magnarello, Bolognini	Initial version
21-03-2016	Sieprawski, Software Mind	Review suggestions
29-03-2016	Massa, Magnarello, Bolognini	Review suggestions
30-03-2016	Janik, Sieprawski	Final version

Contents

1. Summary

The following document provides a general indication of best practices and requirements to ensure the ICT security of SETA. As the SETA technologies and architectures are still to be defined in details, this document is necessarily not addressing any specific solution adopted. It is intended as a guide line to be followed in order to build a secure environment. A detailed audit of SETA environment ICT security will be carried out by M32 and documented in D8.2.3.

2. Glossary of Terms

Annex I	*Otherwise known as the DoW*
CA	*Consortium Agreement*
DoW	*Description of Work*
GA	*Grant Agreement*
WP	*Work Package*

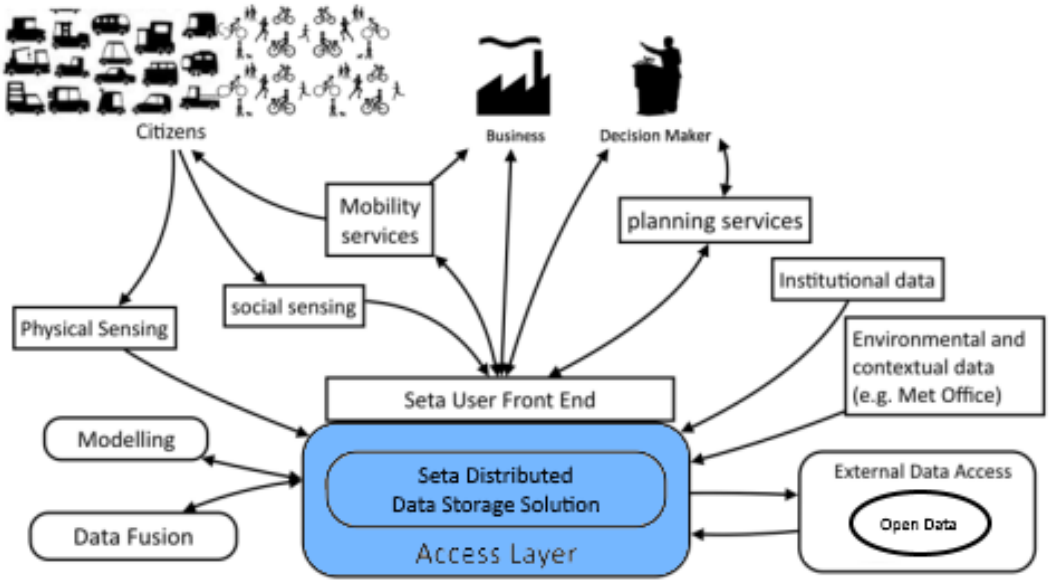
3. Introduction

ICT Security main purposes are to protect data/information and to ensure business continuity. Nevertheless, **security is a cost**, and not every information need to be protected with the maximum level of security available: for example, **no one will spend** a dime **to protect information** that is already **publicly available** on internet.
For this reason, a preliminary analysis of criticality level (low, medium, high) must be performed. This analysis is linked to each service (data) in terms of:

- **Confidentiality**
- **Integrity**
- **Availability**

This is true, especially, for communication from/toward external sources, either physical or virtual.

4. SETA interactions



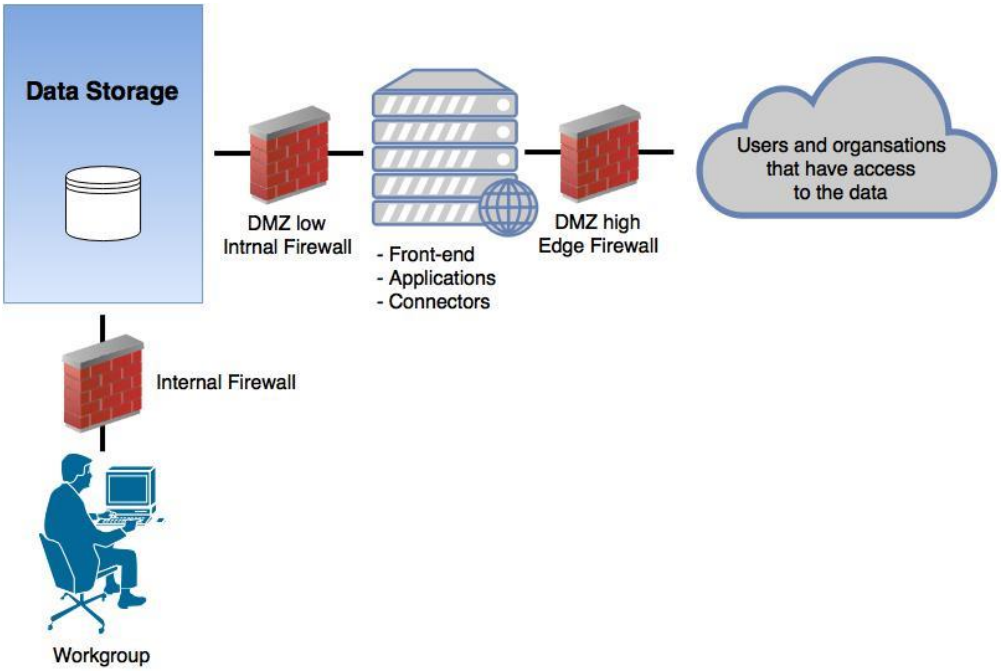
The above is a functional design that describes how the logic components interact between them; SETA is a very complex project, with many different stakeholders interacting with the same data storage in several ways.
For this reason, we chose to apply an access layer that sits between the main storage and those applications who need to access and/or modify data. This way, it is easier to perform access control and rights management.
In order to apply security measures to this conceptual drawing, it is necessary to bring it to a different level of detail. More precisely, we need to split it into two main area:

1) **Trusted area** (in blue): this zone corresponds physically to the data centre where SETA's main systems and data will be installed. By trusted, we mean that here will live only systems kept safe from a security standpoint by means of post installation tasks and periodical update.
2) **Untrusted area**: this zone corresponds to whatever system lives outside the trusted area (user dedicated front-end, Open Data connectors, sensors, etc.).

In the next paragraphs, we will analyse each interconnection between the systems (internal and external), with the final goal of securing the trusted zone.

5. Architecture

Based on the above risk analysis for each protocol and connection needed for SETA, the architecture must adhere to the following security recommendations.
The Data Storage system, containing SETA's data, is considered as a unique box that contains the business core and that, for this reason, must be thoroughly secured.
In order to accomplish this goal, the Trusted Zone must be protected with a firewall from the adjacent Servers will be located in the safe collocation and LAN in Software Mind premises – both connected via dedicated MPLS network, and with a Full Demilitarized Zone (DMZ) composed by High and Low firewalls from everything comes from Internet like shown in the drawing below.



In particular, the DMZ is a physical or logical subnetwork that contains and exposes an organization's external-facing services to a larger and untrusted network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN); an external network node only has direct access to equipment in the DMZ, rather than any other part of the internal network. Also, the DMZ usually includes those services for which it doesn't exist a reverse-proxy able to handle safely the transmission like for example FTP, NTP, etc.

In particular the DMZ for SETA must contain the following tools:

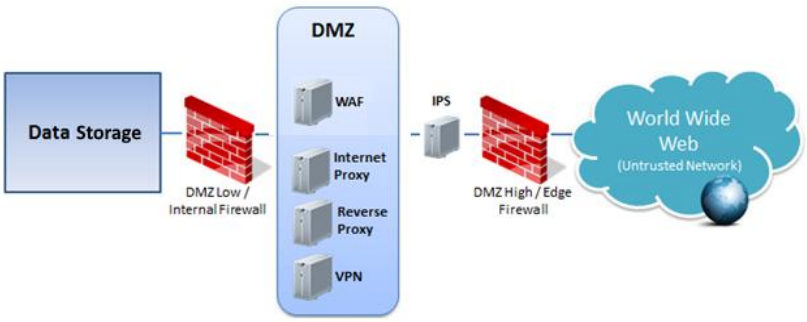
- **WAF:** a web application firewall (WAF) is an appliance, server plugin, or filter that applies a set of rules to an HTTP conversation. Generally, these rules cover common attacks such as cross-site scripting (XSS) and SQL injection. By customizing the rules to your application, many attacks can be identified and blocked. The effort to perform this customization can be significant and needs to be maintained as the application is modified.
- **Forward Proxy/ Internet Proxy:** is an Internet-facing proxy used to retrieve from a wide range of sources (in most cases anywhere on the Internet)

- **Reverse Proxy:** is an Internet-facing proxy used as a front-end to control and protect access to a server on a private network. A reverse proxy commonly also performs tasks such as load-balancing, authentication, decryption or caching.
- **VPN:** software application that implements virtual private network (VPN) techniques for creating secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities.

For those devices that are directly exposed to the internet, IPS is strongly recommended:

- IPS: Intrusion prevention systems (IPS), also known as intrusion detection and prevention systems (IDPS), are network security appliances that monitor network and/or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it. More specifically, IPS can take such actions as sending an alarm, dropping the malicious packets, resetting the connection and/or blocking the traffic from the offending IP address. An IPS can also correct Cyclic Redundancy Check (CRC) errors, unfragment packet streams, prevent TCP sequencing issues, and clean up unwanted transport and network layer options.

Below a picture showing more details of the DMZ area.



5.1. Hardware Security equipment (hypothesis)

5.1.1. Firewalls

We recommend an appliance that combines firewall, application control, intrusion prevention (IPS), P2P security, and web filtering, depending on the complexity of the architecture, those functionalities could be provided by the router. Those would need constant update.

Hardware Security Risks

- Hardware damage (non-redundant hardware components)

OS/Software Security Risks

- Firewall misconfiguration

5.1.2. DMZ Server

Hardware feature

Any service that will be provided to users on the external network will be placed in the DMZ. So SETA will have a DMZ Server that will provide these services.

Security Risks

- Hardware damage (non redundant hardware components)

System Hardening

Hardening is the process of securing a system by reducing its surface of vulnerability. Reducing available vectors of attack typically includes the removal of unnecessary software, unnecessary usernames or logins and the disabling or removal of unnecessary services, installing the latest OS security patches available.

The best practices to improve systems security can be found inside the Center for Internet Security (CIS). It is a not-for-profit organization whose mission is to "enhance the cyber security readiness and response of public and private sector entities, with a commitment to excellence through collaboration."
CIS provides specific guidelines for securing each operative system with different impact level. One of the guidelines, for example, requires setting up operating system firewall security packages like Iptables and SElinux/AppArmor (or similar) enabled if possible (when operating on Linux environments).

5.1.3. Others
The main services installed on the DMZ server will be the Forward-proxy and the Reverse-Proxy software.
A proxy server is a server that acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource available from a different server and the proxy server evaluates the request as a way to simplify and control its complexity. Proxies were invented to add structure and encapsulation to distributed systems. Today, most proxies are web proxies, facilitating access to content on the World Wide Web and providing anonymity
A reverse proxy server is an intermediary. It provides indirect access for an external network (usually the Internet) to internal resources. For example, a back office application access, such as an email system, could be provided to external users (to read emails while outside the company) but the remote user would not have direct access to their email server. Only the reverse proxy server can physically access the internal email server. This is an extra layer of security, which is particularly recommended when internal resources need to be accessed from the outside.

Security Risks
- Operating system misconfiguration/administration
  - Unused Services and Open Ports
  - Unpatched Services
  - Inattentive Administration
  - Insecure Services
  - No local security (local firewall)
  - Virus related issues
- Application related security risks
  - Misconfiguration
  - Unpatching
  - Inattentive Administration
  - AV out of date

5.2. Other hardware related components
Other hardware components inside the SETA infrastructure will include:
- Switches for network connectivity
- Power and network cables
- UPS equipment

This hardware will be provided by Software Mind.
Security Risks
- Hardware damage

5.3. Web Interface
The front-end is probably the easiest way for a hacker to reach the Core Infrastructure, and the most complex connection from/toward external sources, so it must be protected as much as possible.

- The web interface must use secure protocols (HTTPS instead of HTTP). Moreover, only properly authenticated users can access confidential information.

- The web interface must be exposed toward internet by using a Reverse Proxy installed in a full DMZ (high and low firewall) as described in the architecture schema above.

- It is recommended to develop following secure coding guidelines specific for the development language used (https://www.owasp.org/index.php/).

- Authentication: Proper password policies will be set depending on the needs of each service. For the systems which require highest protection/security, the following requisites for password policies will be considered:
    - 8 characters length.
    - Containing a mix of alphabetic and non-alphabetic characters (numbers, digits, punctuation)
    - Expiring after 90 days at most.
    - Not containing the user ID
    - Not containing more than 3 consecutive identical characters.
    - Different from the last 3 passwords used.
- Authorization: once logged into the web application, the users shall be assigned to specific authorization profiles (standard users vs privileged users)
- User management/revalidation: a process for user ID enabling/disabling and a plan for periodical User ID revalidation have to be defined.

It is important to keep the web application as much simple as possible avoiding to develop from scratch new APIs dedicated to services that can be handled in a more efficient and effective way by dedicated server (like an SFTP server, for example).
The more complex the web application is, the more are the chances for a hacker to carry out a successful cyber-attack.
Moreover, we strongly recommend to conduct a Security Penetration Testing of the web application as soon as it will be mature enough.

Security Risks
Website security issues will include:

- Injection
- Broken Authentication and Session Management
- Cross-Site Scripting (XSS)
- Insecure Direct Object References Security Misconfiguration

Risk analysis:

- Probability: 10% - 50%
- Impact: Moderate

5.4. Testing

To face those risks, we recommend to plan testing activities that include vulnerability assessments and penetration testing of the most critical pieces of the infrastructure. Those activities will need to be carried out once the infrastructure is set up completely and ideally before the beginning of the operations.

6. Dataflow hypothesis

Here below, a risk analysis of the different services that we expect to implement into SETA. They are divided into inbound, outbound and local traffic.

- **Inbound flow**: external dataflow that will flow inside SETA Data Storage
- **Outbound flow**: SETA dataflow sent to external resources
- **Internal flow**: dataflow transferred internally between SETA components

6.1. Inbound and Outbound (from/to Internet) flow matrix

The rules of both firewalls will be set to allow the flow of only those TCP/IP protocols/ports and/or subscribed users allowed for the operations of SETA. The following schema will show these protocols/ports:

Service	TC/IP Port	In (from internet)	Out (to Internet)
HTTP server website, HTTP client	TCP 80	Yes	Yes
HTTPS server website, HTTPS client and VPN connections (SSL)	TCP 443	Yes	Yes
SSL-VPN	TBD	Yes	Yes

6.2. Inbound flow analysis

6.2.1. VPN ACCESS – SSL connection

A virtual private network (VPN) extends a private network across a public network, such as the Internet. It enables a computer or network-enabled device to send and receive data across shared or public networks as if it were directly connected to the private network, while benefiting from the functionality, security and management policies of the private network. A VPN is created by establishing a virtual point-to-point connection through the use of dedicated connections, virtual tunnelling protocols, or traffic encryption.

Security risks:
Many weak authentication methods expose the private network to a variety of security attacks. Also, in order to mitigate brute-force attacks, it is common practice to configure account lockout policies after a certain number of wrong login attempts. Nevertheless, this could lead to service unavailability.

Managed by:
- DMZ managed service (firewall)

VPN access will be managed, it will be set up with all users that need to administer, develop or analyze the structure from remote.
Every user will be part of a security access profile (e.g. administrators, ordinary users). Once a user will be authenticate he will have access to all services for which the profile will have permission to, other than to the facilities located in the DMZ zone, also to services located in the network beyond the LOW Firewall like CI and TSI networks.
All the packets through the VPN connection are encrypted.

Security Policy applied:
- account policy with strong passwords for personal certificates keyrings
- account lockout policy

6.2.2. HTTP and HTTPS SERVER

HTTP Protocol
Hypertext is structured text that uses logical links (hyperlinks) between nodes containing text. HTTP is the protocol to exchange or transfer hypertext.
Security risks:

- Clear-text transmission: it means that it is trivial for a man-in-the-middle to analyze the interaction between the client and server in real-time. Can capture cookies used for authentication, login names, passwords and other information passed in forms.
- No certificate: more exposed to phishing attacks and redirection toward untrusted server.
- Stateless protocol: Statelessness makes it much easier for man-in-the middle type attacks

HTTPS Protocol
HTTPS (also called HTTP over TLS, HTTP over SSL, and HTTP Secure) is a protocol for secure communication over a computer network which is widely used on the Internet. HTTPS consists of communication over Hypertext Transfer Protocol (HTTP) within a connection encrypted by Transport Layer Security or its predecessor, Secure Sockets Layer. The main motivation for HTTPS is authentication of the visited website and to protect the privacy and integrity of the exchanged data.
Security risks:

- While HTTPS is the standard for covering the major issues tied to HTTP protocol (like clear text transmission, data integrity, etc.) some residual risks are tied to how strong is the Secure Socket Layer (SSL) used as well as how trustable are the certificate used.

Managed by:

- DMZ reverse-proxy

Incoming connections to http and https webservers will be managed through a reverse-proxy server software installed in the DMZ Server.
It will accept and forward http/https connections to internal servers in the CI and TSI networks.
There will be a multiple antivirus check, on firewalls HIGH and LOW and a virus check on the DMZ server itself. By IPS/WAF service built-in on firewalls we could avoid the typical XSS and Code Injection attacks.

Security Policy applied:

- account policy with strong passwords
- account lockout policy
- multiple antivirus/antispam control
- IPS/WAF inspection

6.3. Outbound flow analysis

6.3.1. HTTP and HTTPS Client

Managed by:

- DMZ forward-proxy
- DMZ URL filtering service

Client connections through http and https protocols are managed directly by built-in HIGH and LOW Firewall URL filtering service.

As far as possible, connections to the outside URLs will be white listed only to certain and specific URLs (e.g. Operating system update sites or well-known sites).

Only specific white listed servers will do http or https traffic to the Internet.

6.4. Local connections

Local connections are connections that remain circumscribed within the facility “TSP premises”. Local connections can be between CI and TSI network and vice versa or from these two networks to the DMZ Server.

They may be involved different TCP/IP protocols, other than those involved in the flow of input and output. We can find for example SSH (management protocol), MySQL communication protocol from client to server etc.
This area can be considered a low risk area because there's not a direct connection from outside (the Internet)
Access to the administrative services of the architecture provided by the cloud service must be accessed with a dedicated VPN, activated by the cloud provider.

6.4.1. Big data database

The client traffic to the Big Data database is only internal between components the SETA network. The LOW firewall will block any access from within or through by this type of protocol. Due to a low risk, traffic between server and clients will not be encrypted.

6.4.2. SSH internal traffic

SSH traffic to manage internal servers (Linux) is a protocol that encrypts all data flowing through it.

It is used for management and it's extremely secure.
Connecting to the servers via SSH will be possible (inside SETA system) with a local connection (sec. 8.4.1 explains it) or through the VPN for remote administration.
It will not be possible to make SSH connections directly from the Internet or to nodes outside the structure "SETA premises", firewalls will block this kind of connections.
To further mitigate the risk you can generate certificates and allow access only through authentication via certificate, the client must have the certificate installed on local.

6.5. Dataflow security matrix

Colour code:
Green: Issues in the green area could be considered at low risk impact
Yellow: Issues in the yellow area could be considered at medium risk
Red: based on the likelihood percentage, issues in this area should be reduced at minimum or mitigated where possible

Consequences **Likelihood**	**Insignificant** (minor problem handled by day to day operation)	**Minor** (some disruption possible)	**Moderate** (significant time/resources requirement)	**Major** (Operations severely damaged)	**Catastrophic** (Business survival at risk)
> 90 %					
50% – 90%	**Inbound** – DMZ (HTTPS)	**Inbound** – DMZ (HTTP)			
10% – 50%			[APP] Website compromised		
3% – 10%		**Outbound** - DMZ (FTP,HTTP/S,NTP) **Outbound** - TRF (HTTP/S)	**Inbound** - DMZ (VPN SSL) **[SW]** – Firewall misconfiguration		
< 3%			**Internal** – Local access for management **Internal** – (MySQL, SSH etc.) **[SW]** DMZ Server operating system malfunctioning **[SW]** DMZ Server – security software malfunctioning (Proxy, reverse proxy, AV)	**[HW]** Firewalls hardware failure **[HW]** Switch failure or network cable related problems	**[HW]** DMZ Server hardware failure(non redundant components)